NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FULL SPECTRUM INFORMATION OPERATIONS AND THE INFORMATION PROFESSIONAL OFFICER INTERMEDIATE QUALIFICATION PROCESS: FILLING THE GAP TO ENSURE THE CONTINUED LEADERSHIP OF THE INFORMATION PROFESSIONAL COMMUNITY IN THE AREA OF INFORMATION DOMINANCE

by

Diego Velasco, Jr.

September 2005

Thesis Advisor:	Daniel C. Boger
Second Reader:	Steven J. Iatrou

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Title (Mix case letters) Full Spectrum Information Operations and the Information Professional Officer Intermediate Qualification Process: Filling the Gap to Ensure the Continued Leadership of the Information Professional Community in the Area of Information Dominance	**5. FUNDING NUMBERS**
6. AUTHOR(S) Diego Velasco, Jr.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

There currently exists a major effort within the United States Navy's Information Professional (IP) Community to overhaul and improve the qualification process for its officers. The overall effort has included the addition of technical refresher courses, re-examination of the Continuing Education Units (CEU) system, and the improvement of the Basic, Intermediate, and Advanced Qualification programs. This thesis specifically addresses the Intermediate Qualification (IQ) and the lack of Information Operations (IO) concepts therein. While some portions of the IQ that address highly technical areas exist, there is little to no mention of the importance of and concepts contained within IO, as defined by Joint Doctrine.

The IP Community has a unique opportunity to train its officers in the concepts, competencies, and supporting activities of IO. This will ensure that the IP Community continues to be the Navy's leaders in the area of information dominance. This thesis provides recommended line items for injection into the IP IQ in the appropriate format with discussions and definitions that address the specific line items. The thesis also provides further recommendations for the continuing improvement and refinement of the IP qualification process, especially in the area of IO.

14. SUBJECT TERMS Information Operations, Information Professional qualifications, IP, IO, Psychological Operations, PSYOP, Electronic Warfare, EW, Military Deception, MILDEC, Operations Security, OPSEC, Computer Network Operations, CNO, Public Affairs, PA, Civil Affairs, CA, Public Diplomacy, PD, IPB	**15. NUMBER OF PAGES** 71
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

FULL-SPECTRUM INFORMATION OPERATIONS AND THE INFORMATION PROFESSIONAL OFFICER INTERMEDIATE QUALIFICATION PROCESS: FILLING THE GAP TO ENSURE THE CONTINUED LEADERSHIP OF THE INFORMATION PROFESSIONAL COMMUNITY IN THE AREA OF INFORMATION DOMINANCE

Diego Velasco, Jr.
Lieutenant, United States Navy
B.A., Tulane University, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Diego Velasco, Jr.

Approved by: Daniel C. Boger
Thesis Advisor

Steven J. Iatrou
Second Reader

Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

There currently exists a major effort within the United States Navy's Information Professional (IP) Community to overhaul and improve the qualification process for its officers. The overall effort has included the addition of technical refresher courses, re-examination of the Continuing Education Units (CEU) system, and the improvement of the Basic, Intermediate, and Advanced Qualification programs. This thesis specifically addresses the Intermediate Qualification (IQ) and the lack of Information Operations (IO) concepts therein. While some portions of the IQ that address highly technical areas exist, there is little to no mention of the importance of and concepts contained within IO, as defined by Joint Doctrine.

The IP Community has a unique opportunity to train its officers in the concepts, competencies, and supporting activities of IO. This will ensure that the IP Community continues to be the Navy's leaders in the area of information dominance. This thesis provides recommended line items for injection into the IP IQ in the appropriate format with discussions and definitions that address the specific line items. The thesis also provides further recommendations for the continuing improvement and refinement of the IP qualification process, especially in the area of IO.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The author would like to gratefully acknowledge those individuals who made this work possible, especially Dr. Daniel C. Boger and Mr. Steven J. Iatrou for their guidance and patience and Dr. Christine M. Brown for her support and counsel.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE OF STUDY

This thesis will serve to promote the injection and inclusion of Full-Spectrum[1] Information Operations (IO) into the Navy's Information Professional (IP) Community's Intermediate Qualification (IQ) Process. The research focused on investigation of the core competencies and supporting activities of IO. The results of the research are line items in the correct format and definitions and answers to the line items. Line items in the IP IQ are individual topics that require signature by personnel who have the required knowledge and expertise to sign them for the IP Officer seeking qualification. The IP Officer must demonstrate proficiency in the topics in order to gain the signatures. Also included in the results of the research are recommendations for the further improvement of the IP IQ Process.

B. BACKGROUND

Information Operations (IO), as defined by Joint Doctrine, are an important part of military strategy, operations, and tactics. IO involve actions taken to affect adversary information and information systems while defending one's own information and information systems (Joint Publication 3-13, 1998: I-1). Under the current definition, there exist five core competencies and various supporting activities within IO. The core competencies are:

- Psychological Operations (PSYOP)
- Military Deception (MILDEC)
- Electronic Warfare (EW)
- Operations Security (OPSEC)

[1] The use and definition of the term "Full-Spectrum" has been defined in different ways and has sometimes been inadvertently misused to limit the overall effectiveness of IO in military operations. In this thesis, the term will be used to signify that IO can and should be used across the full spectrum of military operations (from peace through conflict to peace). The term should not be taken to mean that all competencies of IO must be used in all military operations in order to be effective.

- Computer Network Operations (CNO)[2]

PSYOP are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals (Joint Publication 3-53, 2003: I-1).[3]

MILDEC is defined as being those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (Joint Publication 3-58, 1996: I-1).

EW refers to any military action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack the enemy (Joint Publication 3-51, 2000: I-1).

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems, determine what indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation (Joint Publication 3-54, 1997: I-1).

CNO are those directed against adversary computers and computer networks and toward the protection of friendly computers and computer networks. CNO is subdivided into three areas: Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE).

[2] The latest Joint Publication 3-13 defining IO was released in 1998 and did not include CNO as an IO core competency. However, the "Information Operations Roadmap," approved by the Secretary of Defense on October 30, 2003, includes CNO. The document, which contains numerous recommendations for the next version of Joint Publication 3-13, also refers to Physical Destruction (PHYDEC) as a supporting activity of IO rather than a core competency.

[3] Brief and concise definitions of IO core capabilities and supporting activities are provided here to introduce the concepts. More detailed definitions and discussions are provided in later chapters of this thesis.

Supporting activities include, but are not limited to:

- Public Affairs (PA)
- Civil Affairs (CA)
- Intelligence
- Public Diplomacy (PD)
- Physical Destruction (PHYDEC)

PA are defined as those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense (Joint Publication 3-61, 2005: GL-5).

CA activities are those performed that (1) enhance the relationship between military forces and civil authorities in areas where military forces are present; and (2) involve application of civil affairs functional specialty skills, in areas normally the responsibility of civil government, to enhance conduct of civil-military operations (Joint Publication 3-57.1, 2003: GL-4). Examples may include humanitarian assistance and infrastructure development.

Intelligence is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. It can also be defined as information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (Joint Publication 2-0, 2000: GL-5). The importance of intelligence support to IO cannot be overstated.

According to the US Information Agency's Alumni Association, PD seeks to promote the national interest and the national security of the United States through understanding, informing, and influencing foreign publics and broadening dialogue between American citizens and institutions and their counterparts abroad (USIA Alumni Association, 2002).[4]

[4] Until it was incorporated into the US Department of State in 1999, the US Information Agency was an independent agency within the US government that dealt with foreign affairs and had offices in numerous foreign countries.

PHYDEC is simply defined as the use of “hard kill” weapons against designated strategic, operational, or tactical targets (Joint Publication 3-13, 1998: II-5).

IO, relative to the history of warfare, is a new concept that has only been formally defined for the last ten years. However, most of the elements that make up IO as a whole have been used in all levels of military operations for decades or centuries. The exception is Computer Network Operations (CNO), which are the most recent tools added to the United States’ overall military capabilities. Indeed, the United States Military and Government as a whole are continually endeavoring to fully understand and develop new CNO in support of the national interests.

Apart from CNO, other elements of IO have been used extensively in the past. Psychological Operations (PSYOP) and Military Deception (MILDEC), for example, have been used since the very beginnings of warfare.

The combination of all of the major information-related elements into an overall integrating strategy that is IO has formally existed for less than a decade. During that time, different agencies in the United States Government have embraced the concept while others have been slower in doing so. The United States Navy is currently lagging behind other military services in the incorporation of IO as an integrating strategy. Despite recent significant steps forward (efforts by the Fleet Information Warfare Center, for example), more work needs to be done. The Navy’s Information Professional (IP) Community has a unique opportunity to become the Navy’s leaders in the effective incorporation of IO into all levels of warfare beyond the current emphasis on technical areas.

The current Information Professional Intermediate Qualification (IQ) lacks any mention of IO as defined by Joint Doctrine or any of their core competencies or supporting activities, with the exception of a single line item mentioning Operations Security (OPSEC) and some items on CNO (IQ Requirements for IP Officer, 2004: 56).

This thesis is designed to fill the need for the improvement and incorporation of IO in the IP IQ. It will serve as a valuable input in to the current overall effort to improve the process. It is hoped that the work will aid the IP Community as a whole in understanding and accepting IO as an essential capability in all aspects of operations, both Naval and Joint.

C. BENEFIT OF STUDY

The benefit of the thesis will be the stronger emphasis IO in the IP IQ Process. This will help the overall readiness of the US Navy by ensuring that all IP Officers develop baseline knowledge of IO, which is recognized throughout the United States Military services as an integral and essential capability. IP Officers should gain the knowledge necessary to consider IO in all aspects of planning and operations. The thesis, if ultimately implemented, will allow IP Officers to further develop into the Navy's leaders in the area of US information dominance.[5]

D. RESEARCH QUESTIONS

In exploring the topic of adding IO to the IP IQ, certain questions that needed to be answered arose. In conducting the research, the following questions were specifically addressed:

- How can the use of IO as an integrating strategy be best explained?
- How can the principles of Systems Engineering be best used to develop and produce the required improvements to the IP IQ?
- What format must be used for incorporation of line-items into the most recent IQ?
- What types of training aids are most appropriate for the purposes of aiding the IP Officer in addressing IP IQ line items and what may be currently available?
- What are the best resources for the IP Officer to use to address IO-related line items?
- What further recommendations can be made for the further improvement of the IP IQ Process?

[5] Information Dominance can be defined as the generation, manipulation, and use of information in order to assist in gaining military dominance (Libicki, 1997). IO can be considered a critical military capability in that it aids in the attainment of Information Dominance.

E. SCOPE AND RESEARCH METHOD

The scope of the thesis will be limited to the incorporation of IO into the IP IQ. This effort is not intended to merely add more to the IP IQ, rather it is intended to aid the current effort to streamline and improve the qualification process for IP Officers. Surely, the inclusion of full-spectrum IO into the IP qualification process will ensure that IP Officers have essential knowledge to continue to excel as leaders in the Navy.

IO and the definition of their core competencies and supporting activities continue to be a topic of contention and debate throughout the US Government. However, it is important that IO, in the current definition outlined by Joint Doctrine, be included somewhere in the Navy's training process. The IP IQ is a good starting point for this purpose.

The methodology that was used in this thesis research consisted of the following:

- A literature review of applicable government documents, instructions, books, Joint doctrine and other information sources.
- Working with and seeking advice from appropriate agencies including the Joint Information Operations Center, the Fleet Information Warfare Center, the Naval Network Warfare Command, and the Inter-Agency OPSEC Support Staff.
- The developing of line items that address IO in the correct format and providing associated descriptions, definitions, and training aids.
- Making determinations/recommendations based upon research and analysis.

F. ORGANIZATION OF THESIS

After a discussion of IO and the IP IQ process, the systems engineering process will be covered in order to provide a relevant approach to the research and the inputs to the IP IQ rather than approaching the effort arbitrarily and without a guiding framework.

The thesis will then offer the actual recommended line items and references for injection into the IP IQ. All of the core competencies and many of the concepts and supporting activities of IO will be formally defined and discussed. Line items in the proper format will be offered that will ensure ease of injection into the IP IQ. The items will also be designed to ensure that the qualifying IP Officer is exposed to and well versed in IO.

Finally, conclusions and further recommendations will be offered that are designed to ensure the continued improvement of IO training and education within the IP IQ process.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE IMPORTANCE OF IO AS AN INTEGRATING STRATEGY

A. DISCUSSION

It is not enough to simply identify the elements of IO and treat them as completely separate capabilities that can be used to successfully complete operations. While it is possible to only use one capability, it is essential that the elements of IO be understood as complementary and not mutually exclusive, depending on the circumstances. Two examples illustrate the point.

During OPERATION JUST CAUSE, the 1989 operation that called for the removal on Panamanian dictator Manuel Noriega, tactical PSYOP teams were used. Noriega sought refuge inside the Vatican City embassy compound in an effort to avoid capture by US forces. Loudspeaker teams were utilized to blast loud rock music and messages into the compound, partially in an effort to demoralize Noriega and influence him to surrender. While all efforts, including diplomatic, were used to get Noriega out of the compound, it is widely agreed that the use of tactical PSYOP, without the other elements of IO, was effective. It should be mentioned that loudspeaker messages were not the only PSYOP tools used during the operation. Radio and television broadcasts and leaflets were also utilized in support of the overall objectives (Goldstein, 1996: 270).

While elements of IO can be used alone, in most cases the capabilities can and must be used in conjunction with each other to help accomplish the mission. OPERATION DESERT STORM provides an appropriate example. In an effort to deceive and confuse Saddam Hussein, the US Navy and Marine Corps conducted amphibious exercises in the Persian Gulf. It appeared to Saddam, and many in the international media, that the US would invade Kuwait to expel Iraqi forces via an amphibious operation. Indeed, in the early morning of the amphibious landing, there were many news agencies with cameras and equipment on the beach broadcasting the events live on television. However, the amphibious assault was a ruse. The actual major invasion was to occur from the West and Southwest across numerous miles of desert and through Kuwait into Iraq. While the success or failure of the overall operation did not depend on the success or failure of the deception, it proved to be effective in confusing

Saddam Hussein and influencing him into action (moving troops toward the Kuwaiti shore) and inaction (not moving troops to the areas where the full invasion would occur). The successful deception was supported by different areas of IO including OPSEC, which deals with sensitive but unclassified information. Along with classified items, had too many unclassified pieces of information been released into the public domain, the deception plan might not have succeeded as effectively as it did.

In addition, the use of non-kinetic options (IO tools, for example) could be, depending on the circumstances, preferable to the use of kinetic options. For example, it would be very easy to destroy an adversary's television transmitter with kinetic weaponry. However, if an EW asset could just as easily use directed energy to merely prevent the station from broadcasting, the effectiveness of the station as a vehicle for propaganda would be diminished. Then, either the station could be used by US forces for PSYOP messages targeted at specific influential audiences or it could be taken over by a new and friendly government.

While the use of IO, both when individual competencies are used and when they are used in conjunction with each other, have provided successes, the misuse of the capabilities by not integrating them into the overall effort can cause serious problems. If the IO organization decides to, using an EW asset, render useless a certain frequency on the electromagnetic spectrum that an adversary is using for communications, and that very frequency is being monitored by friendly forces in order to collect valuable adversary information, then an intelligence source will be lost. That, of course, could seriously affect the mission.

Not only must the core elements of IO be taken together to form an integrating strategy, the supporting activities must also be considered. Of course, IO cannot be quite as effective if the intelligence support is not robust or sufficient. In addition, the physical destruction of a target can have a serious psychological and influential effect on an adversary. Civil Affairs have a profound effect in influencing audiences in conjunction with PSYOP campaigns. Indeed, supporting activities to IO are extremely important to consider and utilize, when appropriate.

One of the most contentious issues that arise when considering supporting activities to IO is how Public Affairs (PA) should support IO. Joint doctrine calls for a PA representative to be part of the IO organization within a Joint Force Commander's Staff. The purpose of this representation is for coordination and de-confliction with planned IO activities (Joint Publication 3-13, 1998: IV-6). Often, IO activities like PSYOP are based on themes and messages designed to influence foreign audiences. It is in this area where PA representatives may wish to withdraw from participation and coordination with the IO organization. PA is specifically designed to *inform* domestic and international audiences through media and not *influence*. This difference in semantics alone can cause problems in the coordination of IO activities with PA. However, should PA and PSYOP messages be in direct conflict with each other, serious negative consequences could result.

It is also extremely important to mention that IO, with its core competencies and supporting activities, like all other elements of a plan, should necessarily be conducted in direct or indirect support of the objectives outlined by the Joint Force Commander's overall strategy.

B. IMPORTANCE IN JOINT APPLICATIONS

In recent decades, there has been a trend away from the US military services operating autonomously and toward their operating jointly. From, the creation of the Joint Chiefs of Staff to the current emphasis on Joint Professional Military Education for Officers, the indications are numerous. Still, the military services should maintain some level of autonomy. Every service, after all, has historically had a different mission and different types of assets, tools, and personnel to accomplish it. Tradition is also very important to the individual services. Nevertheless, the trend toward joint operations is a positive one. After all, operations in support of national objectives can usually be more efficiently and effectively accomplished by a force that contains the most appropriate elements of US military power, regardless of what specific military service they come from.

IO, since most effectively used an as integrating strategy, have the potential to be utilized well during Joint operations. The Joint community, as a whole seems to have done well in embracing the concept and importance of IO. Indeed, there exists Joint Doctrine that specifically defines IO, the core competencies, and supporting activities. IO training is conducted at Joint schools such as the Joint Special Operations University in Hurlburt, FL, and the Joint Forces Staff College in Norfolk, VA. In addition, there exist two IO Centers of Excellence, one at the Joint Information Operations Center (JIOC) in San Antonio, TX[6] and one at the Naval Postgraduate School in Monterey, CA. In the area of CNO, the Joint Task Force-Global Network Operations (JTF-GNO) exists to refine existing capabilities and develop new ones while defending friendly networks.

Other organizations that provide IO-related training and support to all US military services and other US government agencies include the Interagency OPSEC Support Staff (IOSS), the Joint Communications Security Monitoring Agency (JCMA), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Defense Intelligence Agency (DIA). There also exist service-specific organizations such as the US Army's 4th PSYOP Group, the Navy's Fleet Information Warfare Center (soon to be Navy Information Operations Command), and the Air Force Information Warfare Center (AFWIC). However, even the service-specific organizations provide support across all military services.

C. IMPORTANCE IN NAVAL APPLICATIONS

Despite the trend toward the US military conducting operations in a joint environment, there are still many instances where the US Navy, either alone or in concert with the US Marine Corps, will be required to conduct operations without the aid of the other military services or other entities. Indeed, the Navy has been known to use elements of IO in the past. An example is the effective use of Electronic Warfare (EW). In fact, the Navy has developed systems and performed modifications to aircraft in order to utilize the EW capabilities to support missions. The EA-6B Prowler aircraft has been

[6] The JIOC provides direct IO support to the Combatant Commander Staffs primarily in the form of deployable teams of general IO experts and specialists. The JIOC also conducts IO training, especially in the area of IO planning.

used during numerous operations to support the mission by jamming enemy radar and communications. The Navy has also developed electronic countermeasures (ECM) designed to oppose enemy weapons systems. In addition, all ships, submarines, and aircraft have specific Emission Conditions (EMCON) postures where emissions from radio, microwave, and other electromagnetic systems are controlled in degrees, depending on the current threat to the platform. Thus, not only is the consideration of IO important in Joint applications, it is also important in Naval applications at all levels of warfare.

Just as in the joint case, the importance and usefulness of IO cannot be overstated. Despite the Navy's history of using certain IO competencies, it is currently struggling to define and implement the concept of IO as a whole. Steps in the right direction have been taken in recent years, however. Efforts by the Fleet Information Warfare Center, especially in the areas of OPSEC training, have had an effect. In addition, the Navy has stepped forward on numerous occasions to support PSYOP campaigns by providing aircraft carrier-based printing and dissemination capabilities for PSYOP products. The recent establishment of the Center for Information Dominance, which combined two information-related activities, is another step in the right direction.

When the Information Professional (IP) community was created, an opportunity presented itself which should not be ignored. Despite the fact that the Cryptology community recently changed its name to Information Warfare and the Navy is taking steps to merge information-related communities[7], there is still no single community that specifically trains its officers in the concepts of full-spectrum IO. The IP Officer Qualification Process, specifically the Intermediate Qualification (IQ), can be a good starting point for ensuring that US Navy Officers have the knowledge and understanding necessary for success as IO-warriors in addition to the expertise in more technical areas currently enjoyed.

[7] A recent indication of this effort is the merging of the Fleet Information Warfare Center (FIWC) Detachment and the Naval Security Group Activity in San Diego, CA. The new combined organization is the Navy Information Operations Command (NIOC), San Diego. Eventually, FIWC Norfolk will be renamed NIOC Norfolk, which will report to the Naval Network Warfare Command, the IP sponsor.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE INFORMATION PROFESSIONAL OFFICER QUALIFICATION PROCESS

A. BACKGROUND

The Information Professional (IP) Community is one of the newest in the US Navy. It was created as a response to the need for a community of officers that would be responsible for certain duties and roles that had been previously under-emphasized or had not existed before the explosion of technology that has occurred over the last few decades. IP Officers are the Navy’s leaders in many important areas. The areas can be separated into two sets of capabilities. The Core Capabilities are Command, Control, Communications, and Computers (C4), Information Technology (IT) Architecture, IT Management and Operations, Communication Systems Management, Computer Network Defense (CND), and Knowledge Management. Special Capabilities include Space Systems Operations, Joint C4, and IT Acquisition. Another set, Functional Area Capabilities, such as Satellite Operations, Tactical Data Link Systems, and Combat Systems, require more specialized knowledge and require more specific training and education.

The IP Officer community was initially populated from various sources within the Navy. Whether it was senior leadership from other officer communities, Limited Duty Officer accession from the senior enlisted ranks, or junior officers being chosen for lateral transfer from warfare communities, varying levels of experience, expertise, and skill populate the IP Officer ranks. In the vast majority of cases, the community has enjoyed the luxury of being able to choose from those officers who apply for selection into it. This gives the IP community a group of leaders that are highly qualified, motivated, and eager to serve to make the community and the Navy, as a whole, better. Eventually, IP Officers will arrive to the community via the Naval Academy, Reserve Officer Training Corp (ROTC) programs, and other paths by which entry-level officers join the Navy.

As in other communities, it is essential that the newest officers complete appropriate training and education in order to gain the knowledge and learn the skills necessary for effective completion of their duties, timely promotion, and continued career success. In addition, continuing education, technical refreshers, and more advanced qualifications are required so that more experienced officers may continue to hone their skills, learn new ones, and succeed. Continuing Education Units (CEU) are required in the IP community on an annual basis, depending on how far the officer is in the qualification process. For example, an officer who has not completed the Intermediate Qualification (IQ) is responsible for fewer annual CEU credits than one who has. This makes sense, of course, since the IQ is a rigorous enough process to warrant the lesser CEU requirement. Along with CEU credits, annual technical refresher training is also required.

The IP community has many and varied resources for their Officers to aid them in their training, education, and qualification. Primarily, the community itself is a close-knit group of people who are eager to help each other. Every entry-level IP Officer is required to identify a sponsor and a mentor -- fellow IP Officers who will aid the newer one in developing as a valued and important member of the community. Additionally, the Navy Knowledge Online (NKO) website (www.nko.navy.mil) is an essential source of relevant and current information pertaining to not only IP training, education, and qualifications, but also IP-related articles, documents, instructions. The IP Detailers also provide links to their areas on the Internet, giving IP Officers an easy way to communicate with and obtain information from them. The website is not limited to IP-related information; it also contains a wealth of information valuable for any Navy member.

B. GOVERNING DIRECTIVES AND REQUIREMENTS

Under the current instructions, there are three distinct levels of qualification for IP Officers: The Basic Qualification (BQ), the Intermediate Qualification (IQ), and the Advanced Qualification (AQ). The governing directive for the IP Qualification Process is Naval Network Warfare Command Instruction (NETWARCOMINST) 1520.1A, dated January 5, 2005. The instruction outlines the requirements that all IP Officers should meet in order to gain and maintain relevant qualification levels. It also delineates timelines and deadlines so that the IP Officer can know at what point in his career path he needs to attain the qualifications.

1. Basic, Intermediate, and Advanced Qualifications

The actual documents that the IP Officer is required to complete are identical to Personnel Qualification Standards (PQS) that have been used in the Navy in the past. In completing the qualification, the IP Officer is required to collect signatures from qualified personnel on numerous line items that have been deemed applicable to the level of qualification the Officer is trying to attain.

Line items are standardized for the Basic and Intermediate Qualification PQS. In other words, all IP Officers must get the same line items signed in order to be eligible for a board of review, which will test the IP Officer on her knowledge of the BQ or IQ areas of emphasis. The Advanced Qualification is slightly different in that the IP Officer may complete it specific to her leadership position and billet in the IP community. The fact that it is different does not make the Advanced Qualification any less important, however.

The BQ is designed to indoctrinate the new IP Officer into the community and expose the new IP to the basics of the designator and the relevant mission areas. The actual line items where signatures are required cover topics including available community resources, IP core and special capabilities, the IP career path, and other items that every new IP Officer should know.

In order to finally gain the BQ and the Additional Qualification Designation (AQD) code associated with it, the IP Officer must stand before a board of qualified reviewers.[8] At the board, the candidate will field questions from the board members in order to demonstrate the knowledge he has gained. In addition, the candidate is required to give a short brief (point paper and visual presentation) addressing an identified problem and recommended solutions. Provided the brief is relevant to IP issues, the candidate may choose any topic he likes. Not only is the portion of the board where the brief is given a good way for the IP Officer to demonstrate knowledge gained, it is also a good way for the candidate to practice and demonstrate verbal skills and display confidence in giving presentations to senior officers. Although the BQ is short,

[8] AQD codes more specifically identify an Officer's qualifications beyond that of the Officer's designator. The AQD for the IP BQ, IQ, and AQ are GA1, GA2, and GA3, respectively.

especially compared to the IQ, it is an effective tool for introducing a new IP Officer to the community and the required knowledge.

In order to help new IP Officers complete the BQ, numerous training aids exist. Some of the most effective aids have been created by other members of the community in an effort to help their peers and those who will follow them in the pursuit of the BQ. For example, IP Officers such as LT Bryan Leatherman, LT Samuel Timmons, and LTJG Michael L. South, have created excellent training aids that have been made readily available to anyone who wishes to use them on the NKO website.

The IQ is much longer and more detailed than the BQ. Rather than the six months given to those pursuing the BQ, three years are allowed to complete the IQ, once the BQ is attained. The IQ is designed to give the IP Officer more extensive knowledge in IP mission areas. As in the BQ, a review board is convened after the candidate gathers all of the required signatures on the line items in the PQS. A point paper and brief are not required.

The IQ is separated into ten modules designed to guide the IP Officer through the process. The modules are designed to be completed in order and are:

- Information Systems Officer
- Communications Officer
- Staff C4I Officer
- Space Officer
- Information Assurance Officer
- Chief Information Officer
- Knowledge Manager
- Information Operations Officer
- C4I Acquisitions Officer
- Combat Systems Officer

Under each module are the line items that require signature by qualified personnel. Included in the modules are instructions for completing various computer-based training courses. The IQ also provides a listing of important acronyms and references.

The AQ is designed to use already existing qualification and certification processes in order to ensure that senior IP Officers are fully qualified and expert in senior IP billets and Navy leadership roles. It is different from other IP qualifications in that it does not have a specific PQS attached to it. In addition, a specific review board does not convene for the IP AQ. Once the IP Officer completes the AQ requirements, she can obtain the AQD.

2. Continuing Education Units (CEU)

The governing directive that outlines the requirements and procedures for the IP CEU program is NETWARCOMINST 1520.2, dated July 25, 2003. The program is important in that it ensures that IP Officers at all levels maintain their technical proficiency and skills. It allows Officers to gain CEU credit in different ways including formal learning experiences such as graduate school courses, participation in professional organizations, and conducting professional activities like writing for a professional journal. The program is very similar to other CEU programs in different fields outside of the military. For example, psychologists must earn annual CEU credits in order to maintain licensure in the states in which they practice. Should they not complete the required amount of CEU credit, they will receive warnings and can eventually lose their licenses (Brown, 2005). The IP CEU program also outlines consequences for the IP Officer who does not complete the requirements on time. Those not in compliance will have the delinquency noted on their Fitness Reports. Such comments, in time, could lead to serious consequences.

CEU credits are recorded and tracked for each IP Officer in NETWARCOM. However, it is the responsibility of the individual Officer to ensure that the proper documentation (transcripts, course completion certificates, etc.) is provided. Luckily, the submission process for CEU credits is easy. An IP Officer wishing to have her CEU credits recorded and tracked can send documents not only via regular mail, but also electronically.

3. IP Annual Technical Refresher Courses

Five refresher courses were developed by the IP Center of Excellence (IPCOE) in conjunction with Kinection, a private contractor. Starting in June, 2005, the courses were made available to the IP community along with a requirement for IP Officers to complete them no later than December 31, 2005. The topics covered by the courses are relevant to the IP community and include C4I (C4 plus Intelligence), Knowledge Management, Satellite Communications, Information Security, and IO. The courses are available on the NKO website's E-learning area. Based on feedback from the IP Community, which is welcomed, the existing courses will be continually improved and new ones developed.

Interestingly enough, the requirement to complete the IO Technical Refresher Course is the first instance where IP Officers have been mandated to receive training in the concepts of IO. The course itself is useful in exposing the IP Officer to some of the broad ideas contained in IO and is a step in the right direction.[9]

C. IQ SHORTCOMINGS AND THE INFORMATION OPERATIONS GAP

An extremely important element in the creation of a new Navy Community is the development of an effective and efficient program to train, educate, and qualify personnel. The IP Community, of course, is no exception. In a remarkably short time, a program, governed by the previously mentioned directives, was developed. Of course, since its inception and initial implementation, the IP Qualification Process has grown and evolved. Numerous improvements have been made to the process. However, work still needs to be done. A serious shortcoming that has been identified is the lack of Information Operations in the qualification process, especially in the IQ, where the injection of IO concepts would be most appropriate.

Other than the IO Technical Refresher Course, and a mention of some IO-related courses in the AQ portion of the IP Qualifications directive, the IP qualification process is almost bereft of IO, despite its importance. There is a module of the PQS that is titled, "Information Operations Officer" and the section opens with a paragraph that makes mention of each IO core competency. However, the twelve line items that follow are

[9] A brief discussion of the IO-related Technical Refresher Course will be provided in the final chapter of this thesis.

highly technical in nature and do not address the definition of IO nor the concepts necessary to understand the concepts of IO. In fact, while one line item in the PQS addresses Operations Security (OPSEC) and one refers to the Fleet Information Warfare Center (FIWC) and the Joint Task Force-Computer Network Defense (JTF-CND), neither of them appears in the IO module.[10]

Despite the serious shortcomings in the IO module, some highly technical concepts dealing with computer networks and electronic warfare are included in some portions of the process. There are also some very IO-relevant line items in the Information Assurance Officer module, although they are also mostly highly technical. However, it is not enough to simply make mention of the technical aspects without providing an understanding of how they fit into the overall concept of IO as an integrating strategy. In addition, it is important to introduce the non-technical concepts of IO and how all of the concepts, competencies, and supporting activities can be utilized together. In short, there is an Information Operations gap within the IP Qualification Process that needs to be addressed.

Probably the best place to address the problem is within the IQ Process. Since the BQ is specifically designed to introduce new IP Officers to the community's vocabulary, roles, and responsibilities, it would not be the most effective place to fully cover IO.[11] The AQ is also not the best step in the process to cover IO. By the time an IP Officer reaches that level, he should already be familiar with IO, especially since it is quite possible that the officer may serve in an IO-related billet during his pursuit of the IQ. Since it is after the introductory and before the advanced qualification, and since enough time is given the IP Officer for its completion, the IQ would be the most appropriate place to address IO.

The IQ has been criticized as being too technical and not operational enough in nature. While this criticism may have merit, the effort that went into the creation of the

[10] JTF-CND became JTF-CNO and has since become JTF-Global Network Operations (GNO). In November, 2005, FIWC will become the Navy Information Operations Command (NIOC).

[11] It may, however, be beneficial to at least introduce IO in the BQ. Since Computer Network Defense is covered as one of the IP core capabilities in the BQ, a mention of CND as an element of IO may be warranted.

IQ should not be discounted. Still, it is commonly accepted within the IP community that the IQ needs continual review and improvement.

IV. THE SYSTEMS ENGINEERING PROCESS

A. INTRODUCTION

Rather than simply produce line items arbitrarily for the injection of some IO concepts into the IP IQ, it is useful to conduct the research and produce the results according to a process that ensures that they will be properly and more efficiently created and eventually utilized. The systems engineering process is useful for this purpose. The process contains principles that aid in the creation of useful ideas that will be developed into effective systems that solve identified problems or requirements. The process also considers systems throughout their entire life cycles including the costs involved. In other words, the systems engineering process considers solutions for identified needs from their inception all the way through development, validation, improvement, maintenance, and finally, disposition.

The systems engineering process in its entirety is extremely useful for the development of complex systems that can take years to develop. Indeed, the process has been used by the US Department of Defense to produce solutions for the needs of the military.[12] Using principles of the process, both complex as well as less scientific solutions to identified requirements can be created.

In researching and developing the incorporation of IO concepts into the IP IQ, certain overarching principles of the systems engineering process proved extremely useful. Using the principles, the research was focused to search for a solution to the identified need. In addition, a "top down" approach was utilized, the life cycle of the solution was considered, and continued improvements to the solution could be addressed for future development.

B. THE OVERALL PROCESS

While different definitions of systems engineering exist, DRM Associates, a firm that provides new product development consulting, offers a useful one:

[12] The Defense Acquisition System utilizes many aspects of systems engineering. An excellent source of information on Defense Acquisition can be found at http://www.dau.mil/.

> The systems engineering process is based on an iterative, top down, hierarchical decomposition of system requirements, supported by trade studies that record the basis for significant decisions and the options considered. The iterative, top-down, hierarchical decomposition methodology includes the parallel activities of Functional Analysis, Allocation, and Synthesis. The iterative process begins with system-level decomposition and then proceeds through the major subsystem level, the functional subsystem level, to the hardware/software configuration item (CI) or assembly/program level [the most basic elements of the system]. As each level is developed, the activities of functional analysis, allocation, and synthesis will be completed before proceeding to the next lower level (DRM Associates, 2005).

Along with application from system-level all the way down to CI level, the process seeks to examine and analyze systems from beginning to end. The process begins with conceptual development where the identification of the need for the system is identified, requirements are analyzed, and further planning takes place. It is also during this phase that the technical approaches to designing the system are evaluated and identified. Important documents such as Operational Requirements Documents (ORD) are produced.

After conceptual development is completed, preliminary design of the system is begun. Trade-off studies are conducted in order to compare different technologies and solutions that fill the requirement and early prototyping is accomplished. Some of the most important documents in the entire process are produced during this phase. The Systems Engineering Management Plan (SEMP), whose purpose is to identify and define the organization, activities, overall tasks, principles, and objectives of system engineering management of the project. The document is used by both the system acquirer and design authority. The Testing and Evaluation Master Plan (TEMP) is also developed at this stage. As the name implies, the TEMP is designed to govern the testing and evaluation of solutions that meet the identified need.

The next step in the process is detailed design and development where construction and engineering of prototypes take place. Further trade-off studies are conducted and production and manufacturing process are verified. The initial planning for full-scale production of the system is also accomplished.

During the production phase, the system and its components are not only made, but also tested and assessed. At this point, further modifications for improvement can be recommended. Despite all of the efficient planning and implementation involved, no system is absolutely perfect.

Once the system or product is distributed for use, the operational and system support phase begins. The performance of the system can be observed in the operational environment and in the hands of the designated users. Regular maintenance and logistic support is performed. Of course, modifications for improvements can continue to be recommended during this time. Feedback from users and designers, always important during the systems engineering process, occurs most during this phase, although it can come in throughout the entire process. Once the system has accomplished what it was designed to do and its life comes to an end, it can be retired (Blanchard and Fabrycky, 1998: 26).

During the entire process, cost is considered. There are costs involved throughout the entire life cycle of the system and its components. From the hiring of contractors to help in the initial planning and concept development, to the personnel who have to dismantle the system for proper disposition, cost across the range of the process must be considered.

Because the solutions offered in this thesis are non-technical in nature, do not carry a great cost, and do not involve the creation of machinery or software, many aspects of the systems engineering process did not prove to be necessary. Still, certain overarching concepts of systems engineering proved to be invaluable in the conducting of research and the development of results.

C. IDENTIFYING THE OPERATIONAL NEED

Identifying a need for a new or improved capability is the first step in the systems engineering process (Blanchard and Fabrycky, 1998: 45). After all, in most cases it may not make sense to expend time, energy, and resources to develop a system if there is not an identified need for it. This seems almost intuitive. However, cases exist in the US military where systems were designed and millions of dollars spent in order to develop them without identified and legitimate needs.

The importance of IO and the need for the incorporation of its concepts into the IP IQ was previously discussed. The research conducted and solutions produced were directly focused to meet the need, taking into consideration the effects of the solution on the overall IP qualification process.

D. UTILIZING A “TOP DOWN” APPROACH

A system can be defined as an assemblage of elements forming a whole (Blanchard and Fabrycky, 1998: 1). For this thesis, research was done and results designed while always keeping the identified requirement in mind. In addition, the IP IQ was treated as a system and the IO module as an element of it. The results of the research – recommended improvements to the IO Module of the PQS -- take into consideration the qualification process as a whole. This approach to designing the solution is part of an overall method in systems engineering known as the “top down” approach. It is characterized by the fact that it can be applied to any part of the system (Blanchard and Fabrycky, 1998: 28). In this case, it was primarily applied to one specific module of the PQS. However, beginning with the system as a whole, the process was applied to smaller and smaller elements of it, namely, the IO module, and then the IO core competencies and supporting activities.

The “top down” approach also aids in design in that it calls for the solution to always be focused on the overall requirement, no matter which element of the system is being designed, maintained, or improved. Indeed, the results of the research for this thesis are specifically designed for improvement of the IP IQ process and ease of incorporation into the overall system.

E. THE LIFE CYCLE AND POTENTIAL FOR FEEDBACK

Too often a complex system is developed considering only its immediate benefits in solving a problem or satisfying a requirement. Post-production costs of maintenance, improvements, and final disposition are not always considered. However, the work and costs involved in the later stages of a system's life cycle are quite important. The systems engineering process considers a system during its complete life cycle (Blanchard and Fabrycky, 1998: 21).

The total life cycle of the results of the research conducted for this thesis was considered despite the fact that they are non-technical in nature. Beyond development and incorporation of the solution, no actual physical maintenance is required. However, after the initial solution, feedback from the IP community is sought and encouraged.

In terms of life cycle cost, the research conducted for and the solutions presented in this thesis are quite cost-effective. The research only involved a review of the existing literature and did not involve any significant costs. Production of the results of the research also involved very little cost. In addition, the incorporation of the results into the IP IQ will cost very little, only involving injecting the recommendations into the PQS and distributing the provided answers and definitions to the IP community. Distribution can easily be accomplished electronically. Continued improvements to the qualification process in the same applicable format will be equally cost-effective.

The motivation behind conducting the research and developing a solution was to add to the overall effort within the IP Community to improve the IP qualification process. Profit was not a consideration. It is hoped that the results of this thesis will be utilized and that the long term benefits of more highly trained and qualified IP Officers will outweigh any of the costs involved.

F. CONTINUED IMPROVEMENTS ON THE INITIAL SOLUTION

The systems engineering process, by virtue of its emphasis on consideration of the full life cycle of a system (inception to death) encourages continual improvement until final disposition. The solution for incorporating IO into the IP IQ is no exception. Based on valuable feedback from the IP community, further technological developments, and changes within IO itself, improvements to the IO Officer Module of the PQS can easily be made. It should be mentioned that any improvements made to the IO Module should always take into consideration the IP IQ as a whole. In other words, revisions and improvements made to the results of this thesis should be made while keeping the overall qualification process in mind.

Feedback, which is also an important part of the systems engineering process, can take different forms in this case. For example, should the recommendations provided in the thesis be implemented, feedback can be observed in the level of IO knowledge displayed by IP Officers in their duties. In addition, direct feedback from the IP community in the form of suggestions and further recommendations for improvement is desired and encouraged. Those responsible for the maintenance of the IP qualification process are available and relatively accessible. Indeed, as of this writing, Naval Network Warfare Command (NETWARCOM), the sponsor of the IP community, has actively solicited the IP community for suggestions to improve the qualification process.

V. IO AND THE CORE COMPETENCIES

A. DISCUSSION

The recommended references, acronyms, and line items that follow address IO on a broad level. They are designed to give the IP Officer some exposure to the concepts and their integration rather than delve too deep into the complexities of IO and IO Planning. The recommended line items are presented here in the order intended for the actual IP IQ PQS and are in bulleted format. This is to preserve the thesis continuity and format. After each bullet, a definition or discussion is provided which is designed to address the line item. The recommended references, acronyms, and line items are presented in the proper format in Appendix A to this thesis.

The IP Officer is encouraged to continue to learn about IO and use the concepts, especially if he can use them to improve the efficiency and effectiveness of his mission accomplishment. As the US military continues to recognize the importance of IO and as more IP Officers are assigned to IO-related billets, the need for the IP community to embrace IO as a war fighting capability will continue to grow.

B. RECOMMENDED REFERENCES

- CJCSI 6520.01D, Information Assurance (IA) and Computer Network Defense (CND). 15 June 2004.

- Joint Publication 3-13, Joint Doctrine for Information Operations. 9 October 1998 (revision in progress).

- Joint Publication 3-51, Joint Doctrine for Electronic Warfare. 7 April 2000.

- Joint Publication 3-53, Joint Doctrine for Psychological Operations. 5 September 2003.

- Joint Publication 3-54, Joint Doctrine for Operations Security. 24 January 1997.

- Electronic Warfare in the Information Age by D. Curtis Schleher. 1999.

- Influence: The Psychology of Persuasion by Robert D. Cialdini, Ph. D. 1993.
- Security in Computing by Charles P. Pfleeger and Shari Lawrence Pfleeger. 2003.

C. RECOMMENDED ACRONYMS

- COMSEC – Communications Security
- CNA – Computer Network Attack
- CND – Computer Network Defense
- CNE – Computer Network Exploitation
- CNO – Computer Network Operations
- EA – Electronic Attack
- EEFI – Essential Elements of Friendly Information
- EP – Electronic Protect
- ES – Electronic Warfare Support
- EW – Electronic Warfare
- GIG – Global Information Grid
- IA – Information Assurance
- IO – Information Operations
- IOSS – Interagency OPSEC Support Staff
- JCMA – Joint COMSEC Monitoring Agency
- JIOC – Joint Information Operations Center
- JRFL – Joint Restricted Frequency List
- JTF-GNO – Joint Task Force, Global Network Operations
- JWRAC – Joint Web Risk Assessment Cell

- MILDEC – Military Deception
- MOE – Measure(s) of Effectiveness
- NIOC – Navy Information Operations Command
- OPSEC – Operations Security
- PSYOP – Psychological Operations

D. RECOMMENDED LINE ITEMS AND DEFINITIONS

1. Information Operations

- Define Information Operations (IO) and discuss their importance.

IO involve actions taken to affect adversary information and information systems while defending one's own information and information systems (Joint Publication 3-13, 1998: I-1).

IO serves as an integrating strategy that can be effectively utilized throughout the entire spectrum of operations from peace through conflict to peace. IO is becoming more widely recognized as an essential element of all military operations.

- List the core competencies and some supporting activities of IO

The five core competencies of IO are Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC). Supporting activities include, but are not limited to, Public Affairs (PA), Civil Affairs (CA), Intelligence, Public Diplomacy and Physical Destruction (PHYDEC).

- Contrast offensive and defensive IO and discuss how different competencies and activities of IO can be utilized together and can support each other.

Offensive IO are used to affect adversary information and information systems and are used to achieve objectives. . Defensive IO are those that are designed to protect and defend friendly information and information systems (Joint Publication 3-13, 1998: viii). Both offensive and defensive IO should employ and integrate all of the necessary elements of IO in order to achieve the intended goal. Examples abound: Information

Assurance (IA) is an overarching concept that incorporates OPSEC, CND, and other defensive capabilities for protection of friendly information. Practicing good OPSEC is an essential part of maintaining the integrity of a MILDEC campaign. Physical destruction typically has a psychological effect on populations and their leaders. PA and PSYOP must be coordinated to ensure that conflicting themes and messages do not reach audiences.

- Discuss IO Measure(s) of Effectiveness (MOE).

The concept of MOE in the realm of IO poses an interesting challenge. Whereas a MOE in a kinetic attack can be as simple as a destroyed target, MOE of a PSYOP or MILDEC are more difficult to observe or quantify. If an adversary takes an action (or inaction) that favors friendly objectives, it is nearly impossible to say with absolute certainty that an IO activity like a PSYOP radio broadcast was responsible for influencing him. On the other hand, it may be quite easy to observe a MOE in the area of CNA or EW in the form of a disrupted website or frequency in the electromagnetic (EM) spectrum. Over the years, the issue of IO MOE has caused much discussion and debate within the US military and Department of Defense, in general, and will continue to do so. Luckily, the difficulty presented has not stopped the US military from continuing to see the validity and importance of IO.

- List some agencies that can aid you in learning about and utilizing IO.

There are many agencies and organizations that provide IO training and direct expert assistance. For the Navy, the primary agency for IO is the Navy Information Operations Command (NIOC) in Norfolk, VA. Under the authority of NETWARCOM and with a detachment in San Diego, CA, the NIOC can provide direct support to Naval forces and staffs and educate personnel in IO concepts.

In the Joint realm, the primary agency for IO is the Joint Information Operations Center (JIOC) in San Antonio, TX. The JIOC primarily provides direct IO support to Combatant Commanders in the form of deployable teams of experts. There also exists an IO Center of Excellence at the Naval Postgraduate School in Monterey, CA that can provide valuable assistance.

The agencies mentioned above also provide IO-related training to personnel. However, there are many other organizations that offer training. For example, the Joint Forces Staff College in Norfolk, VA offers courses like the Joint Information Warfare Staff Officer's Course and a course in Joint IO Planning. The Joint Special Operations University in Hurlburt, FL offers introductory courses in PSYOP. Both the Central Intelligence Agency and Defense Intelligence Agency offer courses in MILDEC.

2. Electronic Warfare

- Define Electronic Warfare (EW) and discuss its importance.

EW refers to any military action involving the use of electromagnetic or directed energy to control the EM spectrum or to attack the enemy (Joint Publication 3-51, 2000: I-1). EW can take many forms at the strategic, operational, and tactical levels of warfare.

With recent technological advances, the field of EW has continued to grow and improve. Along with improvements to current weaponry and defenses that use the electromagnetic spectrum, new tools are constantly being developed. For example, research continues in the field of directed energy weapons (e.g., high energy lasers and charged particle beams) and stealth technology (Schleher, 1999: 472).

- Define and discuss the three elements of EW.

EW is subdivided into three different functionalities: Electronic Attack (EA), Electronic Protect (EP), and Electronic Warfare Support (ES). EA involves the use of energy in the EM spectrum to disrupt, disable, or neutralize adversary electronic systems such as radar or means of communication. The use of electronic jamming to deny the use of certain frequencies of the EM spectrum is an example.

EP involves the use of active and passive measures to protect friendly electronic systems against both adversary and friendly actions. Electronic Countermeasures designed to counter enemy EA or kinetic weaponry guided electronically are examples. The deployment of chaff, which is designed to confuse guided missiles, can be considered an EP measure.

ES involves actions that identify and localize sources of EM energy for the purposes of intelligence collection or targeting.

- Discuss the concept of intelligence loss and how it relates to EW.

An intelligence loss can occur as a result of poor planning and coordination in targeting adversary systems or critical nodes and employing the available kinetic and non-kinetic tools in military operations. For example, should an EA be conducted against a frequency or channel that is being monitored by friendly forces for collection of important adversary information, an intelligence loss occurs. While the example is not the only possible instance of intelligence loss, it illustrates how IO (EW in this particular case) must be fully integrated and coordinated in order to avoid conflict. Fortunately, mechanisms and procedures exist that aid in the avoidance of intelligence loss. For example, the Joint Restricted Frequency List (JRFL) outlines which frequencies in the EM spectrum are not to be disrupted during a Joint operation.

3. Computer Network Operations

- Define Computer Network Operations (CNO) and discuss their importance.

CNO are those directed against adversary computers and computer networks and toward the protection of friendly computers and computer networks. CNO can be subdivided into three areas: Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE).

With the recent explosion in technology, most of the world's important systems are driven by computers. The Department of Defense is no exception. More than ever before, the DoD is dependent on automation and computer technology. Indeed, along with unclassified computer networks, classified networks have also been created and without them, the organization's effectiveness will be severely hampered. It has been discovered that, in recent years, defense-related computer systems have been targeted by domestic and international individuals and organizations. Thus, not only must the US do what it can to protect essential computers and computer networks, information about the threats should be collected via computers and methods should be developed to counter the threats. As far as the US military is concerned, in addition to network defense, it is also important to develop tools for the collection of adversary information and the possible attack on adversary computer systems.

- Discuss the three elements of CNO and the difficulties involved in conducting each.

CNA can be defined as the use of computers and computer networks to disrupt, deny, manipulate, or otherwise actively affect an adversary's computers or computer networks. Due to the global nature of the Internet and computer networks, getting approval to conduct CNA is very difficult. After all, it is very possible that a CNA will inadvertently affect other friendly systems. In addition, some countries consider a CNA an act of war.

CNE consists of gaining access to adversary computers and computer networks for the purposes of intelligence collection. CNE seeks to find adversary vulnerabilities and important information that will aid friendly forces. There is difficulty in drawing definite boundaries between CNA and CNE. As technology improves and the nature of computer systems becomes more global, the debate will continue and the lines will continue to be blurred (CJCSI 6510.01D, 2004: GL-9).

CND is interested in protecting friendly computers and computer networks. Not only do proper defenses need to be employed, but also constant vigilance in the form of detecting unauthorized access or intrusions. In recent years, Department of Defense computer systems have been actively probed and attacked. Those responsible can be motivated by things such as fame, power, money, or ideology and use many different methods to affect friendly systems. Attacks can take the form of interception, interruption, modification, and fabrication (Pfleeger, 2003: 7).

- Identify some CNO-related organizations within the Department of Defense.

The Joint Task Force, Global Network Operations (JTF-GNO) is the agency responsible for the operation and defense of the Global Information Grid (GIG). In addition, Computer Incident (or Emergency) Response Teams exist to monitor US military computer networks and alert appropriate agencies when problems occur. Network Operations Centers also aid in the overall CNO effort.

4. Psychological Operations

- Define Psychological Operations (PSYOP) and discuss their importance.

PSYOP are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals (Joint Publication 3-53, 2003: I-1).

PSYOP has existed and has been used for centuries in different forms. The US has used PSYOP during numerous military operations and at all levels of warfare. For example, PSYOP was used at the tactical level during OPERATION DESERT STORM by dropping leaflets on Iraqi forces in an effort to convince them to surrender to coalition forces. Many of the troops that actually surrendered were carrying the leaflets.

All PSYOP products are designed to support the overall themes and messages developed at the strategic level which, in turn, support the overall objectives of the mission commander. In addition to leaflets, PSYOP can also consist of television and radio broadcasts, and published articles.

- Discuss a few of the major PSYOP missions.

PSYOP units and forces serve some important functions in support of the overall mission. First, they advise the commander during the planning process on many of the psychological considerations that should be considered during the operation. Second, they work to influence foreign populations into action (or inaction) to support friendly objectives. PSYOP forces provide public information to public audiences in support of humanitarian activities and to assist in restoring and maintaining civil order. They also serve as the voice of the commander to foreign audiences and work to counter adversary propaganda. Coordination with Public Affairs (PA) is essential in the successful accomplishment of these missions (Joint Publication 3-53, 2003: I-5).

- What is a target audience? Discuss different types and why it is important to know the psychological/sociological attributes of target audiences.

A target audience is an individual or group selected for influence or attack by means of PSYOP (Joint Publication 3-53, 2003: GL-9). A target audience can be a specific adversary decision maker or a large segment of a foreign population. PSYOP forces seek to know the culture, biases, and psychological/sociological attributes of target audiences to properly tailor themes and messages directed to them. This gives the PSYOP effort the ability to manipulate unwitting audiences. “Even the victims themselves tend to see their compliance as determined by the action of natural forces rather than by the designs” of the people who profit from them (Cialdini, 1993: 11).

5. Military Deception

- Define Military Deception (MILDEC) and discuss its importance.

MILDEC is defined as being those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (Joint Publication 3-58, 1996: I-1).

MILDEC has been used for centuries and in different forms. A good MILDEC can convince an adversary that forces are greater than they actually are or that a friendly force will attack somewhere that is actually will not.

In recent history, the US has used MILDEC effectively. One of the best examples that illustrate this point is the success of the strategic MILDEC campaign against Iraqi leadership during OPERATION DESERT STORM. The overall campaign was designed to convince Saddam Hussein that the US would invade Kuwait and Iraq via amphibious assault. The US conducted military maneuvers and coordinated with other agencies to relay observable indicators to Iraqi leadership. The fact that Hussein placed forces on the Kuwaiti and Iraqi coasts to defend against a US assault demonstrated that he believed that that it would happen. However, despite the fact that some US forces did land amphibiously, the major push toward Iraq was conducted over land from Saudi Arabia into Western Iraq.

MILDEC, when successfully and carefully planned, can do much to support the overall objectives of a mission. However, it is extremely important to mention that the success or failure of a mission should never depend wholly on the success or failure of a MILDEC. IO planners should always take this into consideration when creating a MILDEC campaign.

Any MILDEC can be supported by any or all of the other IO core competencies, particularly OPSEC and PSYOP. Normally, a MILDEC campaign, even at the tactical level, is appropriately classified and distribution of the plan is limited.

- Discuss the steps in the overall MILDEC Planning Process

There are six sequential steps in the MILDEC planning process. Deception Mission Analysis involves examining how a deception can support the overall mission. Deception Planning Guidance is then given by the commander of the operation. A Staff Deception Estimate is then conducted. In this step, all available information about the adversary including intentions, psychological profiles, and cultural considerations, is collected and considered. The planners assess the feasibility of conducting a deception campaign, given the available information and different deception courses of action are developed. The Commander's Deception Estimate is the part of the process where the commander chooses a course of action (or none at all, depending on the circumstances). Deception Plan Development, the most time consuming part of the process is then conducted. Plan development is detailed and exhaustive and consists of completing the deception story, identifying the means, developing the event schedule, identifying feedback channels, and developing the termination concept. Finally, Deception Plan Review and Approval is conducted by the commander (Joint Publication 3-58, 1996: IV-3).

6. Operations Security

- Define Operations Security (OPSEC) and discuss its importance.

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems, determine what indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation (Joint Publication 3-54, 1997: I-1). The practicing of OPSEC is the responsibility of all personnel and every major military command should have an OPSEC Program Manager. It is important to note that OPSEC deals with the protection of sensitive *unclassified* information.

OPSEC is not meant to be the only tool used for the security of an operation. Rather, it is meant to supplement other ongoing security efforts such as the protection of classified information, computer network security, and physical security.

- Describe the five steps in the OPSEC process and give examples of Essential Elements of Friendly Information (EEFI), Critical Information, OPSEC indicators, and OPSEC measures.

The OPSEC process consists of five sequential steps: Identification of Critical Information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC measures (Joint Publication 3-54, 1997: III-2).

EEFI are identified as the questions that a potential adversary would like the answers to in order to find out about our capabilities, intentions, and activities. Critical Information is a subset of EEFI and is defined as the most vital information needed by an adversary (Joint Publication 3-54, 1997: III-1). In order to use the rest of the OPSEC process in the protection of Critical Information, it must first be actually identified.

Analysis of threats involves learning as much as possible about adversaries and what they can use against us in terms of information gathering. It is also important to know what the adversary already knows about us.

Analysis of vulnerabilities involves thoroughly examining the command or operation and seeking OPSEC indicators, which are those actions and fragments of information that an adversary might piece together to gain valuable insight into friendly activities, capabilities, and intentions (Joint Publication 3-54, 1997: C-1). It is important to identify and understand the vulnerabilities so that they may be appropriately addressed.

Risk assessment involves understanding the actual risk posed by the adversary in exploiting an identified vulnerability. Should enough a risk be deemed to exist, then appropriate OPSEC measures must be chosen.

The last step, of course, is the actual implementation of the chosen OPSEC measures. Measures should be created and tailored to the specific vulnerabilities.

However, some examples of OPSEC measures that can generally be used include administrative ones like concealing budgetary transactions that would reveal preparations for activity and operational ones like avoiding repetitive tactics and procedures (Joint Publication 3-54, 1997: D-1).

- List some agencies or resources that can aid you in learning about and using the OPSEC process.

The Interagency OPSEC Support Staff (IOSS) was created under the National Security Decision Directive (NSDD) 298, which established a national OPSEC program. The IOSS is a valuable source of information and offers training courses that range from training in fundamentals to advanced applications classes. Products such as videotapes and posters designed to aid the OPSEC practitioner and manager are also offered. The IOSS can be reached at www.ioss.gov. In addition, the IOSS can send experts to a command to conduct a full OPSEC survey, which is a comprehensive review of policies and practices.

Other agencies that offer assistance in the practice of good OPSEC include the Joint COMSEC Monitoring Agency (JCMA), Navy Information Operations Command (NIOC), Joint Information Operations Center (JIOC), and Joint Web Risk Assessment Cell (JWRAC). JCMA offers electronic and telephonic monitoring in order to help commands identify problems in their OPSEC practices. NIOC and JIOC can aid commands by conducting OPSEC surveys, often in conjunction with the IOSS. The JWRAC monitors Department of Defense websites for inadvertent releases of sensitive information.

VI. IO SUPPORTING ACTIVITIES

A. RECOMMENDED REFERENCES

- Joint Publication 2-0, Doctrine for Intelligence Support to Joint Operations. 9 March 2000.
- Joint Publication 3-57.1, Joint Doctrine for Civil Affairs. 14 April 2003.
- Joint Publication 3-61, Public Affairs. 9 May 2005.
- Strategic Public Diplomacy and American Foreign Policy: The Evolution of Influence by Jarol B. Manheim. 1994.

B. RECOMMENDED ACRONYMS

- PA – Public Affairs
- CA – Civil Affairs
- CMO – Civil-military Operations
- IPB – Intelligence preparation of the battlespace
- NGO – Non-governmental Organization
- PD – Public Diplomacy
- PHYDEC – Physical Destruction

C. RECOMMENDED LINE ITEMS AND DEFINITIONS

1. Public Affairs

- Define Public Affairs (PA) and discuss their importance.

PA are defined as those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense (Joint Publication 3-61, 2005: GL-5).

American society has very rigid mores concerning the people's right to know. Despite the fact that certain essential pieces of information are classified and only available to those with the appropriate level of clearance and the “need to know,” the US military, through PA, takes measures to ensure that domestic audiences stay informed. In addition, PA seek to inform international audiences through media outlets. During OPERATION IRAQI FREEDOM, daily press conferences for the media and embedded journalists within actual military units demonstrated the resolve of PA efforts to keep the public informed.

It is important to mention the differences between PA and PSYOP. While PSYOP are designed to influence audiences, PA seeks to inform. However, PSYOP efforts and PA should be coordinated to avoid contradictions in messages that go out to various audiences. Should the PA and PSYOP efforts be in direct conflict, consequences ranging from simple embarrassment to the breakdown of a coalition could result.

- Discuss the three basic functions of PA.

There are three basic functions of PA: Public Information, Command/Internal Information, and Community Relations (Joint Publication 3-61, 2005: III-3).

With recent advances in technology, information is more easily accessible and widely available to audiences across the globe. Despite this fact, the US military must continue to work with domestic and international media outlets in order provide information regarding operations to the public. In addition, it is important to keep internal military audiences like deployed forces, local military personnel, and their families informed. Publications like newspapers specific to military bases and command websites are examples of how PA can keep internal audiences apprised. Finally, PA functions to aid in community relations as a whole by developing and maintaining amicable dealings between the US military presence in a community and the community itself. The relationship is especially important when military forces are deployed away from the area they would otherwise inhabit.

- Identify and discuss the target audiences of PA efforts.

First, PA efforts are directed toward the American Public. Promptly and faithfully informing the US public about the military and current operations builds and supports a relationship of trust. Maintaining that relationship is important for continued public support of and confidence in the US military.

Second, international audiences are targeted by PA efforts. The global nature of media and information dissemination almost necessarily means that any information given to American audiences will reach international audiences as well. In addition, it is important to inform foreign audiences when there is a US military presence in their country.

Third, PA address internal audiences like military personnel and their families. This aids in building a relationship between military members and their commanders.

Finally, adversary forces are targeted by PA. Information designed to inform domestic and international audiences could possibly affect the morale of the forces, their commanders, or other key decision makers. Of course, when it comes to affecting adversary forces, PA should coordinate with any PSYOP efforts, as appropriate.

2. Civil Affairs

- Define Civil Affairs (CA) and discuss their importance in supporting IO.

CA activities are those performed that (1) enhance the relationship between military forces and civil authorities in areas where military forces are present; and (2) involve application of civil affairs functional specialty skills, in areas normally the responsibility of civil government, to enhance conduct of civil-military operations (Joint Publication 3-57.1, 2003: GL-4). CA activities are performed to support civil-military operations (CMO), which establish relationships between the US military and other organizations like civilian governments and non-governmental organizations (NGO). CMO and CA can be conducted prior to, during, and after military operations. Examples of CA activities may include humanitarian assistance and infrastructure development or reconstruction.

CA can support IO in numerous ways. For example, the rebuilding of critical infrastructure in a foreign country after a military conflict can help ease tensions between the local population and US forces. This type of positive influence can help support ongoing PSYOP and PA efforts. In addition, relationships developed and maintained between the US military and civilian organizations can help all elements of an operation run more smoothly, including IO.

3. Intelligence

- Discuss intelligence preparation of the battlespace (IPB) and the importance of intelligence support to IO.

Intelligence is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. It can also be defined as information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (Joint Publication 2-0, 2000: GL-5). There are many sources of intelligence including human beings, satellite imagery, electronic signals, and Internet research.

Intelligence preparation of the battlespace (IPB) refers to the collection of all necessary intelligence to aid in the successful accomplishment of the mission. The collected information can be examined to discover enemy vulnerabilities, terrain data, and other pertinent items that will aid in planning and executing the operation. All of the data can be placed into a large database for easy access. The continuing IPB process helps in reducing uncertainty (Joint Publication 3-13, 1998: GL-8).

The importance of intelligence support to IO cannot be overstated. Since IO can be used throughout all levels of warfare, accurate and timely intelligence at each level is essential. Intelligence products that directly support IO include, but are not limited to, psychological profiles of key adversary decision-makers, computer network infrastructure information, and information concerning adversary denial and deception programs.

4. Public Diplomacy

- Define Public Diplomacy (PD) and discuss its importance in supporting IO.

According to the US Information Agency's Alumni Association, PD seeks to promote the national interest and the national security of the United States through understanding, informing, and influencing foreign publics and broadening dialogue between American citizens and institutions and their counterparts abroad (USIA Alumni Association, 2002). PD is not normally specifically conducted by the US military.

Rather, PD efforts are conducted by other organizations and entities such as the US Department of State. However, it is important to consider ongoing PD efforts in planning and executing IO in support of a US military operation. Just as in the case of PSYOP and PA, if efforts were not coordinated properly and vastly different messages were put out by different agencies, the overall credibility of the US would be diminished in the eyes of foreign audiences.

- List some examples of activities that can be considered PD.

Many examples of activities that can be considered PD exist. For example, foreign student/teacher exchange programs such as the Fulbright Program seek to promote mutual understanding among different peoples. US Embassies in foreign countries also conduct activities that promote US cultural values and ideals. The Voice of America (VOA), which was created in 1942 to counter Nazi propaganda, is used for PD purposes. Finally, some libraries are maintained overseas by the US Information Service (Manheim, 1994: 5).

5. Physical Destruction

- Define Physical Destruction (PHYDEC) and discuss how it can support IO efforts.

PHYDEC is simply defined as the use of "hard kill" weapons against designated strategic, operational, or tactical targets (Joint Publication 3-13, 1998: II-5). Prior to recent revisions, PHYDEC was included as a core competency of IO in the Joint Publication 3-13. However, despite the fact that it is now considered a supporting activity, PHYDEC is no less important as a tool that can be used to enhance IO.

The destruction of a target can have a psychological effect on adversary decision makers, their forces, and their populations. In addition, PHYDEC can be used to support IO by affecting specific targets as part of a larger system. For example, rather than simply obliterating targets at random, destroying a target that denies the adversary critical communications abilities can be even more damaging on the whole.

Another benefit of coordinating PHYDEC efforts with IO is the prevention of intelligence losses. Just as in the case of Electronic Attack, a PHYDEC can destroy a target that was previously being used to gather intelligence. This situation should be avoided through proper coordination.

VII. SUMMARY AND RECOMMENDATIONS

A. SUMMARY

More than ever before, IO is being recognized as essential to military operations at all levels of warfare. IO, due to its importance and nature as an integrating strategy, has been accepted by the US Department of Defense and the US Navy as a critical capability that should be utilized to the fullest extent whenever appropriate.

The IP community, one of the US Navy's newest, has a unique opportunity to become the Navy leaders and experts in the realm of IO. The IP qualification process is a good place to begin. This thesis offered recommendations for the incorporation of IO into the IP IQ Process, particularly the PQS that all IP Officers are required to complete. The intent was not to simply add more work to the process for the IP Officer. Instead, the results of the research are offered as an input to the ongoing community-wide effort to review and streamline the entire IP qualification system. The overall thesis and the research conducted to complete it followed a systems engineering approach to ensure that a viable and effective framework was used. It is hoped that the recommendations will be accepted by the IP community leadership and utilized to help the IP community as a whole continue to be the Navy leaders in the area of total Information Dominance.

B. FURTHER RECOMMENDATIONS

The scope of this thesis was limited to the IP IQ Process. However, there are other areas within the IP Officer qualification and continuing education process where the concepts of IO can effectively be incorporated. This, of course, will ensure that the IP community continues to be the Navy leader in the area of information dominance.

As mentioned earlier, a step in the right direction was taken when one of the annual technical refresher courses was made mandatory for all IP Officers. The course, Coordinating the Elements of Information Operations (IO), is available online and can be completed in about an hour. It is a good tool for exposing the IP Officer to the concept of IO and effectively presents examples of how IO has been utilized in the past. It also provides interesting scenarios in which the IP Officer can think about and use some of the concepts. Based on feedback from those who have taken the course, which is highly encouraged and welcome, the course will be refined and any minor issues will be addressed. It is hoped that the recommendations presented in this thesis will serve to replace the course as the initial exposure to IO for the IP Officer. Then the technical refresher will be just that: a refresher.

Another step in the right direction is the inclusion of IO-related training courses into the IP continuing education process. Indeed, as of this writing the document that shows approved courses for Continuing Education Units (CEU) makes mention of the Joint Information Warfare Staff and Operations Course (JIWSOC) and Joint IO Planning Course (JIOPC) offered by the Joint Forces Staff College and the Naval Information Warfare Staff and Operations Course (NIWSOC) offered by the Fleet Information Warfare Center (FIWC). However, numerous other IO-related courses exist that should be included in the IP CEU program.

The Interagency OPSEC Support Staff (IOSS) offers excellent courses that deal with OPSEC. The most basic course offered is the OPSEC Security Fundamentals Course which is a computer-based training available for order from the IOSS. Courses offered at the IOSS schoolhouse include the OPSEC Program Manager’s Course, the Web Risk Assessment Course, and the OPSEC Advanced Applications Course.

Both the Defense Intelligence Agency (DIA) and the Central Intelligence Agency (CIA) offer courses in adversarial denial and deception. In addition, the DIA offers courses in intelligence support to IO. The Joint Information Operations Center offers a course in Joint IO Planning. Courses in PSYOP are offered by the Joint Special Operations University. Indeed, all of the courses mentioned above can easily be included in the IP CEU program and would offer more options for IP Officers to meet their annual requirements and add to their levels of expertise. With more highly trained personnel, the IP Community and Navy, as a whole will benefit.

The IP Community is slowly recognizing that its personnel should be trained in the concepts of IO. However, it is in the author’s opinion that a stronger emphasis needs to be placed. Along with the incorporation of IO into the IP IQ and CEU Programs, IO should be considered a core capability along with the current ones (C4, IT Architecture, Communications Systems Management, etc.).

Finally, more IO-related billets should be identified and assigned to IP Officers, especially in the area of strategic IO planning ashore and operational and tactical planning at sea. The author recognizes that this recommendation is much easier suggested than accomplished, but considers it an important one to mention.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

ACRONYMS USED IN THIS IQ

COMSEC	Communications Security
CA	Civil Affairs
CMO	Civil-military Operations
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
EA	Electronic Attack
EEFI	Essential Elements of Friendly Information
EP	Electronic Protect
ES	Electronic Warfare Support
EW	Electronic Warfare
GIG	Global Information Grid
IA	Information Assurance
IO	Information Operations
IOSS	Interagency OPSEC Support Staff
IPB	Intelligence preparation of the battlespace
JCMA	Joint COMSEC Monitoring Agency
JIOC	Joint Information Operations Center
JRFL	Joint Restricted Frequency List
JTF-GNO	Joint Task Force, Global Network Operations
JWRAC	Joint Web Risk Assessment Cell
MILDEC	Military Deception
MOE	Measures of Effectiveness
NGO	Non-governmental Organization
NIOC	Navy Information Operations Command
OPSEC	Operations Security
PA	Public Affairs
PD	Public Diplomacy
PHYDEC	Physical Destruction
PSYOP	Psychological Operations

References: (a) Joint Publication 3-13, Joint Doctrine for Information Operations. 9 October 1998.
(b) Joint Publication 3-51, Joint Doctrine for Electronic Warfare. 7 April 2000.
(c) Joint Publication 3-53, Joint Doctrine for Psychological Operations. 5 September 2003.
(d) Joint Publication 3-54, Joint Doctrine for Operations Security. 24 January 1997.

(e) Electronic Warfare in the Information Age by D. Curtis Schleher. 1999.
(f) Influence: The Psychology of Persuasion by Robert D. Cialdini, Ph. D. 1993.
(g) CJCSI 6520.01D, Information Assurance (IA) and Computer Network Defense (CND). 15 June 2004.
(h) Security in Computing by Charles P. Pfleeger and Shari Lawrence Pfleeger. 2003
(i) Joint Publication 3-61, Public Affairs. 9 May 2005.
(j) Joint Publication 3-57.1, Joint Doctrine for Civil Affairs. 14 April 2003.
(k) Joint Publication 2-0, Doctrine for Intelligence Support to Joint Operations. 9 March 2000.
(l) Strategic Public Diplomacy and American Foreign Policy: The Evolution of Influence by Jarol B. Manheim. 1994.

8. **INFORMATION OPERATIONS OFFICER**

- Plans, directs, coordinates and supports all aspects of Information Operations (IO) (Electronic Warfare (EW), Operations Security (OPSEC), Psychological Operations (PSYOP), Military Deception (MILDEC) and Computer Network Operations (CNO)) across the organization
- Provides IO guidance and policies to C4I operations at strategic, operational and tactical levels

801. **INFORMATION OPERATIONS FUNDAMENTALS**

Refer to reference (a).

801.a Define Information Operations (IO) and discuss their importance.

____
Signature Date

801.b List the core competencies and some supporting activities of IO.

____
Signature Date

801.c Contrast offensive and defensive IO and discuss how different competencies and activities of IO can be utilized together and can support each other.

____
Signature Date

801.d Discuss IO Measure(s) of Effectiveness (MOE).

____
Signature   Date

801.e List some agencies that can aid you in learning about and utilizing IO.

____
Signature   Date

802. **INFORMATION OPERATIONS CORE COMPETENCIES**

Refer to references (b) through (h)

802.a Define Electronic Warfare (EW) and discuss its importance.

____
Signature   Date

802.b Define and discuss the three elements of EW.

____
Signature   Date

802.c Discuss the concept of intelligence loss and how it relates to EW.

____
Signature   Date

802.d Define Computer Network Operations (CNO) and discuss their importance.

____
Signature   Date

802.e Discuss the three elements of CNO and the difficulties involved in conducting each.

____
Signature   Date

802.f Identify some CNO-related organizations within the Department of Defense.

Signature Date

802.g Define Psychological Operations (PSYOP) and discuss their importance.

Signature Date

802.h Discuss a few of the major PSYOP missions.

Signature Date

802.i What is a target audience? Discuss different types and why it is important to know the psychological/sociological attributes of target audiences.

Signature Date

802.j Define Military Deception (MILDEC) and discuss its importance.

Signature Date

802.k Discuss the steps in the overall MILDEC Planning Process.

Signature Date

802.l Define Operations Security (OPSEC) and discuss its importance.

Signature Date

802.m Describe the five steps in the OPSEC process and give examples of Essential Elements of Friendly Information (EEFI), Critical Information, OPSEC indicators, and OPSEC measures.

____

Signature   Date

802.n List some agencies or resources that can aid you in learning about and using the OPSEC process.

____

Signature   Date

803. **<u>INFORMATION OPERATIONS SUPPORTING ACTIVITIES</u>**

Refer to references (i) through (l)

803.a Define Public Affairs (PA) and discuss their importance.

____

Signature   Date

803.b Discuss the three basic functions of PA.

____

Signature   Date

803.c Identify and discuss the target audiences of PA efforts.

____

Signature   Date

803.d Define Civil Affairs (CA) and discuss their importance in supporting IO.

____

Signature   Date

803.e Discuss the importance of intelligence support to IO.

____

Signature   Date

803.f Define Public Diplomacy (PD) and discuss its importance in supporting IO.

Signature Date

803.g List some examples of activities that can be considered PD.

Signature Date

803.h Define Physical Destruction (PHYDEC) and discuss how it can support IO efforts.

Signature Date

LIST OF REFERENCES

Blanchard, Benjamin S. and Wolter J. Fabrycky. Systems Engineering and Analysis. 3rd Ed. Upper Saddle River, NJ: Prentice-Hall, 1998.

Brown, Christine M, Clinical Psychologist, Correctional Training Facility, Soledad, CA. Telephone Interview. 13 Jul. 2005.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01D, Information Assurance (IA) and Computer Network Defense (CND). 15 Jun. 2004.

Cialdini, Robert B. Influence: The Psychology of Persuasion. New York: Quill William Morrow, 1993.

DRM Associates, "Systems Engineering Process." <http://www.npd-solutions.com/se.html > [24 Aug. 2005]

Goldstein, Frank L., Ed. Psychological Operations: Principles and Case Studies. Maxwell Air Force Base, AL: Air University Press, 1996.

The Joint Chiefs of Staff. Joint Publication 3-13, Joint Doctrine for Information Operations. Washington, DC, 1998.

The Joint Chiefs of Staff. Joint Publication 3-51, Joint Doctrine for Electronic Warfare, Washington, DC, 2000.

The Joint Chiefs of Staff. Joint Publication 3-53, Joint Doctrine for Psychological Operations. Washington, DC, 2003.

The Joint Chiefs of Staff. Joint Publication 3-54, Joint Doctrine for Operations Security. Washington, DC, 1997.

The Joint Chiefs of Staff. Joint Publication 3-57.1, Joint Doctrine for Civil Affairs. Washington, DC, 2003.

The Joint Chiefs of Staff. Joint Publication 3-58, Joint Doctrine for Military Deception. Washington, DC, 1996.

The Joint Chiefs of Staff. Joint Publication 3-61, Public Affairs. Washington, DC, 2005.

The Joint Chiefs of Staff. Joint Publication 2-0, Doctrine for Intelligence Support to Joint Operations. Washington, DC, 2000.

Libicki, Martin C. "Information Dominance" Nov. 1997. <http://www.ndu.edu/inss/strforum/SF132/forum132.html> [9 Sep. 2005]

Manheim, Jarol B. Strategic Public Diplomacy and American Foreign Policy: The Evolution of Influence. Oxford: Oxford University Press, 1994.

Naval Network Warfare Command Instruction 1520.1A, Active Duty Information Professional Officer (160X) Qualification Program. 5 Jan. 2005

Naval Network Warfare Command Instruction 1520.2, Active Duty Information Professional Officer (160X) Continuing Education Unit Program. 25 Jul. 2003

Pfleeger, Charles P. and Shari Lawrence Pfleeger. Security in Computing. Upper Saddle River, NJ: Prentice Hall, 2003.

Schleher, D. Curtis. Electronic Warfare in the Information Age. Norwood, MA: Artech House, 1999.

US Secretary of Defense. "Information Operations Roadmap." Washington, DC, 2003.

USIA Alumni Association. "What is Public Diplomacy?" 1 Sep. 2002. <http://www.publicdiplomacy.org/1.htm> [16 Aug. 2005]

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Naval Network Warfare Command
   Virginia Beach, Virginia

4. Information Professional Center of Excellence
   Naval Postgraduate School
   Monterey, California

5. Dan C. Boger
   Naval Postgraduate School
   Monterey, California